

ORIGINAL

FILED IN CHAMBERS  
U.S.D.C. Atlanta

**United States District Court**  
NORTHERN DISTRICT OF GEORGIA

NOV 14 2014

JAMES N. HATTEN, Clerk  
By: DRG Deputy Clerk

UNITED STATES OF AMERICA

v.

**CRIMINAL COMPLAINT**

DAVID DA SILVA

Case Number: 1:14-MJ-1012  
(Under Seal)

I, the undersigned complainant being duly sworn, state the following is true and correct to the best of my knowledge and belief. Beginning on an unknown date, but at least by in or about February 2009 through in or about June 2012, in the Northern District of Georgia and elsewhere, the defendant, **David Da Silva**, did knowingly combine, conspire, and agree with other persons known and unknown to commit offenses against the United States in violation of Title 18, United States Code, Section 1956, to wit:

(a) to knowingly conduct and attempt to conduct a financial transaction affecting interstate and foreign commerce, which involved the proceeds of a specified unlawful activity, that is, wire fraud, in violation of Title 18, United States Code, Section 1343, and computer fraud, in violation of Title 18, United States Code, Section 1030, with the intent to promote the carrying on of specified lawful activity, that is, wire fraud and computer fraud, and that while conducting and attempting to conduct such financial transaction knew that the property involved in the financial transaction represented the proceeds of some form of unlawful activity in violation of Title 18, United States Code, Section 1956(a)(1)(A)(i); and

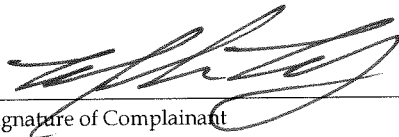
(b) to knowingly conduct and attempt to conduct financial transactions affecting interstate and foreign commerce, which transactions involved the proceeds of specified unlawful activity, that is, wire fraud, in violation of Title 18, United States Code, Section 1343, and computer fraud, in violation of Title 18, United States Code, Section 1030, knowing that the transactions were designed in whole or in part to conceal and disguise the nature, location, source, ownership, and control of the proceeds of specified unlawful activity, and that while conducting and attempting to conduct such financial transactions, knew that the property involved in the financial transactions represented the proceeds of some form of unlawful activity, in violation of Title 18, United States Code, Section 1956(a)(1)(B)(i).

All in violation of Title 18, United States Code, Section 1956(h).

I further state that I am a Special Agent with the Federal Bureau of Investigation ("FBI") and that this complaint is based on the following facts:

PLEASE SEE ATTACHED AFFIDAVIT

Continued on the attached sheet and made a part hereof. Yes

  
\_\_\_\_\_  
Signature of Complainant  
MARK C. RAY

Based upon this complaint, this Court finds that there is probable cause to believe that an offense has been committed and that the defendant has committed it. Sworn to before me, and subscribed in my presence

November 14, 2014

Date

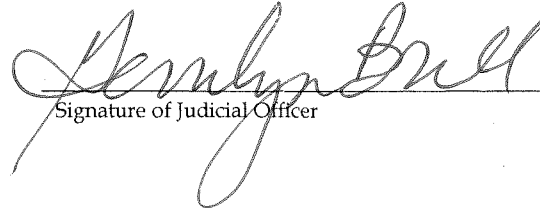
at Atlanta, Georgia

City and State

GERRILYN G. BRILL  
UNITED STATES MAGISTRATE JUDGE

Name and Title of Judicial Officer

AUSA Steven D. Grimberg / 2014R00058

  
Signature of Judicial Officer

**AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT**

I, Mark C. Ray, being first duly sworn, hereby depose and state as follows:

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been since February 2010. I am currently assigned to the Atlanta Field Office Cyber Crimes squad. My current duties include the full-time investigation of computer crimes, and I have participated in numerous investigations involving computer and high technology related crimes including computer intrusions, Internet fraud, and credit card fraud. I have also received specialized training in the federal criminal statutes that relate to computer intrusions and other computer-related crimes, and in the investigation of these offenses. Moreover, I am an investigative or law enforcement officer of the United States, and as such I am empowered to conduct investigations of and to make arrests for offenses enumerated in 18 U.S.C. § 1956 (laundering of monetary instruments); 18 U.S.C. § 1957 (engaging in monetary transactions in property derived from specified unlawful activity); and for other federal felony offenses.

2. Prior to joining the FBI, I worked for over twelve years in the private sector, specializing in computer and Information Systems ("IS") related work. During that time, I gained extensive experience in computer programming, computer operating, and managing computer software systems.

**PURPOSE OF THE AFFIDAVIT**

3. I make this affidavit in support of the issuance of a Criminal Complaint and Arrest Warrant against **David Da Silva** ("**Silva**"), who is believed to be a Canadian citizen currently residing in Canada. The purpose of this affidavit is to establish probable cause for **Silva's** arrest for conspiracy to commit money laundering, in violation of Title 18, United States Code, Section 1956(h).

4. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information I obtained from various law enforcement agents and others. Because this affidavit is being submitted for the limited purpose of establishing probable cause, I have not included in this affidavit every detail of every aspect of the investigation. Rather, I have set forth facts that I believe are sufficient to establish probable cause for the issuance of the requested Criminal Complaint and Arrest Warrant. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

#### BACKGROUND

##### *Email Service Providers*

5. Between February 2009 and June 2012, at least eight Email Service Providers (“ESPs”), including two ESPs in the Northern District of Georgia, experienced unauthorized accesses into their computer systems. ESPs are companies that are legitimate senders of bulk emails. Generally, clients of ESPs contract with ESPs in order to send email marketing messages to the clients’ customers who have opted-in to receive such correspondence. ESPs specialize in developing technology and partnerships that allow them to deliver a higher percentage of bulk emails through the spam filters of Internet Service Providers (“ISPs”) than their clients could achieve on their own.

6. The unauthorized accesses resulted in the unauthorized downloading of confidential customer lists and the unauthorized distribution of bulk emails. The unauthorized emails promoted fraudulent schemes such as enticing the recipients to web sites selling free software; in other words, an unwitting customer would pay the cybercriminal who controls the

web site for products normally offered for free by a legitimate company. The unauthorized emails also distributed malicious computer software by sending targeted messages containing links to malware.

### ***Hacking Conspirators***

7. On October 3, 2012, a Federal Grand Jury in the Northern District of Georgia returned an indictment against Viet Quoc Nguyen and Giang Hoang Vu in relation to their alleged unauthorized access into the ESPs as described above. Nguyen and Vu were charged with a wire fraud conspiracy, among other offenses. Vu was arrested and extradited to the United States from the Netherlands on March 14, 2014. Vu's case is currently pending. Viet Nguyen is believed to reside in Vietnam but is not in custody.

### ***Affiliate Marketing***

8. One scheme by which the computer intrusions at the ESPs by Nguyen and Vu were monetized involved affiliate marketing.

9. Affiliate marketing is a type of marketing business in which persons or companies, known as affiliates, enter into marketing agreements with companies to generate sales of their products. Affiliates earn commissions on sales to customers who purchase the products from websites associated with the affiliate.

10. To maximize their revenue, affiliate marketers need to generate large volumes of Internet traffic to affiliate marketing websites. In order to generate this traffic, affiliate marketers require large volumes of valid e-mail addresses, the means to send a high volume of e-mails to these e-mail addresses, and the ability to ensure that these e-mails would not be classified as spam by their recipient's e-mail programs.

11. The FBI has determined that Nguyen engaged in affiliate marketing to monetize the large volumes of email addresses he obtained through his hacking offenses. Specifically, Nguyen was an affiliate marketer who received a percentage of any sales from traffic he directed to specific websites. Some of the unauthorized e-mail campaigns conducted by Nguyen directed recipients to these specific websites, and thus, Nguyen received commissions for sales generated at the websites.

***MarketBay***

12. The FBI obtained a search warrant for the email account vnlzone@yahoo.com believed to be controlled by Nguyen. FBI analysis indicated that the vnlzone@yahoo.com email account appeared to contain, among other emails, approximately 160 emails from December 17, 2009 through October 17, 2011 between Nguyen and an affiliate marketing company named MarketBay.

13. One of the emails found was dated August 25, 2010, and was sent from "Affiliate Manager contact@marketbay.com" to "Viet Nguyen <vnlzone@yahoo.com>". The email listed several web sites, to include the web site www.new-tv-to-pc.com, and stated that the web sites were "hardcoded" to Nguyen's affiliate ID. In my training and experience I believe this to mean that any sales generated from the web site www.new-tv-to-pc.com would result in sales commissions exclusively for Nguyen. The vnlzone@yahoo.com included other emails that indicated that Nguyen similarly promoted approximately 55 other web sites on marketbay.com.

14. In response to a MLAT issued in or about April 2011 from the United States Department of Justice to the Competent Authority of the Netherlands, Netherlands law enforcement provide bank account records for Nguyen. Analysis of these records indicate that Nguyen made approximately \$1.5 million from MarketBay via affiliate marketing.

PROBABLE CAUSE

***“Jake” at MarketBay Had Knowledge of Nguyen’s Hacking Activities***

15. FBI analysis of the contents of the vnlzone@yahoo.com email account indicates that at least one MarketBay employee was aware that Nguyen was using fraudulent methods to direct large volumes of internet traffic to his affiliate marketing websites and helped facilitate his activities. Of the approximately 160 emails between Nguyen and MarketBay from December 17, 2009, through October 6, 2011, approximately 128 emails were signed using the name “Jake” (“Jake emails”) to include the August 25, 2010 email referenced in paragraph 13 above.

16. On multiple occasions Nguyen informed Jake about his hacking and spamming activities. For example, on December 7, 2010, Nguyen informed Jake that:

“I have a good news , somehow i just got data from 16.000.000 Skype Users , yes 16 millions skype users with type ; Email, Skype ID”

17. And on July 12, 2011, Nguyen informed Jake that:

“i still have so much email database from almost all big company of the world and i need your help to get as much as sales from them.”

18. On August 13, 2014, Nguyen’s alleged co-conspirator, Giang Vu, was interviewed by United States law enforcement. Vu stated that Nguyen showed Vu how to make money by sending spam to stolen email lists in order promote MarketBay products. Nguyen helped Vu to become a MarketBay affiliate.

19. Nguyen described himself as a MarketBay employee to Vu. Nguyen told Vu that Nguyen was a top seller at MarketBay, that MarketBay knew that Nguyen promoted his products through spam, and that no person could sell as many products as Nguyen did through legitimate

means. Nguyen also told Vu that MarketBay invited Nguyen to travel to Canada to meet with them, that MarketBay wanted Nguyen to work for MarketBay corporate, and that MarketBay wanted Nguyen to bring his stolen email lists with him to MarketBay.

***David Da Silva is Jake***

20. Email headers associated with the Jake emails indicate that the emails were sent from IP address 69.70.55.234 ("Jake IP 1") from December 17, 2013, through October 6, 2011. During this time frame the Jake emails were sent from two separate computers during distinct time ranges. From December 17, 2009 through June 14, 2010 the Jake emails were sent from a computer identified as "575e8a3fafde44f". From June 30, 2010 through October 6, 2011, they were sent from a computer identified as "DavidPC". Other information stored in the email headers to include language (en-us), mailer (Outlook 12), and timezone (Eastern) were consistent throughout the Jake emails. I believe that this consistent association of the Jake emails with two computer names over distinct date ranges indicates that a single individual was responsible for the Jake emails and that this individual likely changed computers between June 14, 2010 and June 30, 2010.

21. The FBI located other emails in the vnlzone@yahoo.com email account whose email headers indicated that they were sent from a computer identified as "575e8a3fafde44f". This included at least seven emails from "Jake <contact@yourclick.com>" to vnlzone@yahoo.com. The email headers for these seven emails indicate that from August 14, 2009, through November 24, 2009, the computer identified as "575e8a3fafde44f" was assigned IP address 69.70.139.158 ("Jake IP 2"). The FBI has determined that yourclick.com is a predecessor to MarketBay and that Jake was Nguyen's point of contact at both affiliate marketing programs.



22. On two occasions the Jake emails were signed using the name David instead of Jake. On September 27, 2010, an email was sent from [contact@marketbay.com](mailto:contact@marketbay.com) to [vnlzone@yahoo.com](mailto:vnlzone@yahoo.com) and signed "David". This email was in reply to several previous emails between [contact@marketbay.com](mailto:contact@marketbay.com) and [vnlzone@yahoo.com](mailto:vnlzone@yahoo.com) that were signed as "Jake". On April 21, 2011, an email was sent from [jake@marketbay.com](mailto:jake@marketbay.com) to [vnlzone@yahoo.com](mailto:vnlzone@yahoo.com) and was signed "David".

23. As the Jake emails appear to be principally sent from a computer identified as "DavidPC", and as on two occasions the name David was used to sign emails otherwise appearing to involve an individual named Jake, I believe that it is likely that the name Jake is an alias being used by an individual named David to communicate with Nguyen.

24. The FBI obtained a search warrant for the email account [david@8sphere.com](mailto:david@8sphere.com) believed to be controlled by **Silva**. One of the emails was sent on August 20, 2010, from "Affiliate Manager <[contact@marketbay.com](mailto:contact@marketbay.com)>" to [david@8sphere.com](mailto:david@8sphere.com). This email contained the body "TO DO" followed by a forwarded email from "Viet Nguyen <[vnlzone@yahoo.com](mailto:vnlzone@yahoo.com)>." Based on my training and experience I believe **Silva** was forwarding an email from Jake's email account, which **Silva** controlled, to **Silva's** email account.

25. In an email sent on March 29, 2011, from "David Da S. <[david@8sphere.com](mailto:david@8sphere.com)>" to [Robert@markeybay.com](mailto:Robert@markeybay.com), with the subject "affiliate list," **Silva** states "Hi Robert, Here is my list." **Silva** subsequently lists several affiliate IDs to include 13340, the affiliate ID for Nguyen. Robert responds in part "That's about it. These are the only people from that list that have contacted me, other than Viet who I already knew was one of yours and have forwarded everything from him to you."

26. In the david@8sphere.com email account the FBI found approximately 33 references to “575e8a3fafde44f.” For example, an email sent on June 16, 2010, from “David <david@8sphere.com>” included an email header indicating the email had been sent from a computer named “575e8a3fafde44f.”

27. In the david@8sphere.com email account the FBI found approximately 187 references to “DavidPC.” For example, an email sent on August 17, 2010, from “David da S. <david@8sphere.com>” included an email header indicating that the email had been sent from a computer named “DavidPC.”

28. An email sent on September 25, 2013, from david@8sphere.com included in part:

My question is that as of August 2012 the following 2 people stopped receiving a paycheck from our company 21 Celsius:

Giuseppe Jr Bruno  
David Manual Da Silva (myself).

We are the 2 owners of the company.

Thanks,

David

29. The investigation has determined that 21 Celsius is a parent company to MarketBay. Based on the above I believe that **Silva** is a co-owner of MarketBay, and that **Silva** is Jake.

### CONCLUSION

30. Based on the above, I believe that **Silva** knew that the affiliate marketing activity conducted by Nguyen involved the unlawful use and monetization of stolen email lists. While having knowledge of these unlawful activities, **Silva** enabled Nguyen’s affiliate marketing

activities, which resulted in over \$1.5 million in revenue for Nguyen and approximately \$375,000 in revenue for MarketBay.

31. Based upon the foregoing, your affiant attests that there is probable cause to believe that **David Da Silva** engaged in a conspiracy to commit money laundering in violation of 18 U.S.C. § 1956(h).

32. Further, your affiant respectfully requests that an arrest warrant be issued for the immediate arrest of **David Da Silva**.